CNS-105-2 Critique #6 : Attack against Tor

B03901027　徐彥旻

Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services

一、攻擊方法

1. Threat model

攻擊者是網路管理者或網路供應商，或者是 Malicious Entry Guard。能夠看到網路部分的封包。在這樣的假設之下，攻擊者能夠取得正確的封包資訊，並且能分辨看到的封包是屬於哪一條迴路。

2. Approach

製作出能利用各個中繼所蒐集到的封包資訊（時間戳記、封包方向與數量、迴路的活動時間等等），進行分類的分類器，這個分類器要能夠區分出經過中繼的迴路是屬於 client-IP、 HS-IP、 client-RP、 HS-RP 或是一般網路溝通的哪一種。

如此一來，便能夠由分類結果來推斷 hidden service 與 hidden service user 可能的位置。換言之，這兩種人所處的 anonymity set 大小將大幅下降，匿名性會遭到削減。

這樣的攻擊能夠成立的條件，是 hidden service 使用的迴路不像一般的 tor 迴路，是不會重複交錯的，並且 hidden service 的頁面隨時間改變的程度較不劇烈，不會隨著使用者所在地區做客製化（至少最一開始連的頁面不會）。才能夠讓分類器有足夠高的正確率。

3. Experiments

研究者自行架設 client 與 hidden service，這些自行架設的 hidden service 是較熱門隱藏服務的快取，模擬使用者連線的情形，蒐集訓練模型用的資料。

實驗的結果相當成功，表現最好的 C4.5 每個類別的辨識正確率都有 95% 以上。

二、可能的防禦

- 所有的迴路都應該要有相似的活動時間（active time），client 跟 introduction point 連接的迴路活動時間過短，非常容易被分類器辨識。
- 基於同樣的理由，隱藏服務應該要每 400-800 秒重新與 introduction point 做連結，以免活動時間過長，容易被分類器辨識。
- introduction point 所在的迴路應該要有更大量的封包經過（原本進出都是 3-4 個 cell）。
- 如果以後 tor 真的改成只有一個 entry guard，那麼所有的迴路都應該要是成對的，而不只有是在連 hidden service 的時候是如此。